A Decoding Failure Test for the Transform Decoder of Reed-Solomon Codes

R. L. Miller and T. K. Truong
Communications Systems Research Section

I. S. Reed
Department of Electrical Engineering
University of Southern California

Using a finite field transform, a transform decoding algorithm is able to correct erasures as well as errors of any (n, k, d) Reed-Solomon code over the finite field GF(q). This article discusses a pitfall of transform decoding and how to avoid it. A simple test is given so that the decoder will fail to decode instead of introducing additional errors, whenever the received word contains too many errors and erasures.

I. Introduction

Voyager, Galileo, and International Solar Polar Mission (ISPM) each have the capability to employ a coding scheme consisting of a (7, 1/2) convolutional inner code concatenated with a (255, 223) Reed-Solomon outer code. A Reed-Solomon decoding algorithm capable of correcting both errors and erasures was described in Ref. 1. This algorithm is called "transform decoding," since it resembles the Fast Fourier Transform (FFT). This feature allows an efficient software implementation. An additional advantage to transform decoding is that it is amenable to analysis by Fourier methods. This article proposes a modification of the algorithm which will essentially eliminate decoding mistakes.

Consider any (n, k, d) Reed-Solomon (RS) code over $GF(q)$ Ref. 2. Then any combination of s erasures and t errors can be corrected if $2t + s < d$. In the event that $2t + s \geq d$, it is desirable to have the decoder respond with a decoding failure, i.e., with an alarm telling of the inability to decode. Unfortunately, in some cases it is also possible for a decoding error to occur; this will happen if the received word is incorrectly decoded, thereby yielding the wrong code word.

Berlekamp and Ramsey (Ref. 3) showed that for the case $s + 2t = d + 1$, a lower bound to the probability of incorrectly decoding using any algorithm is given by

$$\binom{n-s-t}{t-1}(q-1)-(t-1)$$

Recently, a simplified algorithm was developed (Ref. 1) for correcting erasures and errors of RS codes over $GF(q)$, using the finite field transform method. In this article, it is shown that with transform decoding, decoding errors will always occur if $s + 2t \geq d$, unless proper care is taken.

II. Transform Decoding Algorithm

Suppose that $c(X)$ is transmitted and $r(X) = c(X) + e(X)$ is received, containing s erasures at locations $\{Z_1, Z_2, \ldots, Z_s\}$

and t (unknown) errors. Then transform decoding of the (n, k, d) Reed-Solomon code generated by

$$g(x) = \prod_{i=1}^{d-1} (x - \alpha^i)$$

(where α is a primitive n^{th} root of unity) consists of the following steps:

Step 1. Compute the syndromes:

$$S_j = r(\alpha^j) \text{ for } 1 \leqslant j \leqslant d - 1 .$$

Step 2. Compute the erasure locator polynomial:

$$\tau(X) = \prod_{j=1}^{s} (X - Z_j) = \sum_{j=0}^{s} (-1)^j \tau_j X^{s-j} .$$

Step 3. Compute

$$T_i = \sum_{j=0}^{s} (-1)^j \tau_j S_{i+s-j} \quad \text{for } 1 \leqslant i \leqslant d - 1 - s .$$

Step 4. Compute the error-locator polynomial

$$\sigma(X)$$

from

$$T_1, \ldots, T_{d-1-s}.$$

See Ref. 4 for details.

Step 5. Compute

$$\mu(X) = \sigma(X)\tau(X) = \sum_{i=0}^{s+t.} (-1)^i \mu_i X^{s+t-i} .$$

Step 6. Compute the "extended" syndromes by

$$S_l = \sum_{i=1}^{s+t} (-1)^i \mu_i S_{l-i} \quad \text{for } d \leqslant l \leqslant n .$$

Step 7. Compute the error-erasure pattern

$$e(X) = \sum_{i=1}^{n-1} e_i X^i,$$

by

$$e_i = \frac{1}{n} S(\alpha^{-i}),$$

where

$$S(X) = \sum_{l=0}^{n-1} S_l X^l,$$

and

$$S_o = S_n .$$

Step 8. Decode $r(X)$ to yield $c(X) = r(X) - e(X)$.

III. A Transform Decoding Pitfall

This section discusses the proclivity of a transform decoder for making its own errors instead of flagging as uncorrectable a received word containing t errors and s erasures, when $2t + s \geqslant d$. It will be shown in the next theorem that a transform decoder does its task perhaps a little too well.

Theorem 1

The output of a transform decoder will always be a code word, regardless of the input.

Proof

Suppose that

$$f(X) = \sum_{i=0}^{n-1} f_i X^i$$

is input to the decoder, and

$$e(X) = \sum_{i=0}^{n-1} e_i X^i$$

is the output of Step 7 in the decoding algorithm. Then $h(X) = f(X) - e(X)$ will be a code word for the following reason. If $1 \leqslant j \leqslant d - 1$, then

$$h(\alpha^j) = f(\alpha^j) - e(\alpha^j)$$

$$= S_j - e(\alpha^j) \quad \text{by Step 1.}$$

But,

$$e(\alpha^j) = \sum_{i=0}^{n-1} e_i \alpha^{ij}$$

$$= \sum_{i=0}^{n-1} \frac{1}{n} S(\alpha^{-i}) \alpha^{ij} \quad \text{by Step 7}$$

$$= \frac{1}{n} \sum_{i=0}^{n-1} \left(\sum_{l=0}^{n-1} S_l \alpha^{-il} \right) \alpha^{ij}$$

$$= \frac{1}{n} \sum_{l=0}^{n-1} S_l \sum_{i=0}^{n-1} \alpha^{(j-l)i}$$

$$= S_j, \text{ since the inner sum vanishes unless } j = l.$$

Thus, $h(\alpha^j) = S_j - e(\alpha^j) = 0$ for $1 \leqslant j \leqslant d - 1$, and $f(X) - e(X)$ is a code word.

IV. A Simple Method for Detecting Decoding Errors

The previous theorem indicates that a transform decoder will allow errors to go undetected in the decoding process unless care is taken. The method to be presented here allows the decoder to detect when it makes a mistake, whenever it is theoretically possible. There are instances, as described in Ref. 3, when no decoder can detect that it has erred. For example, if $d - 1$ erasures occur, then the decoder will "correct" those positions yielding a code word, no matter how many additional errors are present. The next theorem provides a test so that decoding failures can be declared instead of allowing the decoder to output bad data unknowingly. Of course, when a decoding failure occurs, the best policy is to leave the received word unaltered.

Theorem 2

Suppose that t errors and s erasures have occurred, and that the Hamming weight of the error vector computed by the decoder is w. Then the decoder has erred if $2w \geqslant d + s$.

Proof

The decoder errs whenever $2t + s \geqslant d$. Unfortunately, t is unknown; only s and d are known by the decoder. Now since $w = t + s$, if

$$2t + s \geqslant d,$$

then

$$2(w - s) + s \geqslant d,$$

hence

$$2w \geqslant d + s.$$

References

1. Reed, I. S., and Truong, T. K., "A Simplified Algorithm for Correcting Both Errors and Erasures of R-S Codes," *Deep Space Network Progress Report 42-48*, September and October 1978, Jet Propulsion Laboratory, Pasadena, Calif., Dec. 15, 1978.

2. McEliece, R. J., *The Theory of Information and Coding*, Addison-Wesley, London, 1977.

3. Berlekamp, E. R., and Ramsey, J. L., "Readable Erasures Improve the Performance of Reed-Solomon Codes," *IEEE Trans. Information Theory*, Vol. IT-24, No. 5, Sept. 1978.

4. Reed, I. S., Scholtz, R. A., Truong, T. K., and Welch, L. R., "The Fast Decoding of Reed-Solomon Codes Using Fermat Theoretic Transforms and Continued Fractions," *IEEE Trans. Information Theory*, Vol. IT-24, No. 1, Jan. 1978.